Outline

- Agents
- Applications
- Concerns
- Information Assurance
- Summary

Agents and Information Assurance

Protecting Machines from Agents
and Agents from Machines

Patrick Lincoln

SRI International
333 Ravenswood Avenue
Menlo Park CA 94025

http://www.csl.sri.com/~lincoln

What is an Agent?

Mobile Agents

Programs that move among computer hosts

Autonomous Agents

Based on planning technologies

Learning Agents

User preferences, collaborative filtering,...

Animated Interface Agents

Avatars, chatbots, ...

Simulation-based Entities

Cooperative Agents

Collaboration among distributed heterogeneous components

Examples

Voyager, Aglets, Odyssey

Robots, Softbots

FireFly, MIT Media Lab

Microsoft Agent, Julia

ModSAF, RoboCup

OAA, KQML, FIPA

Main Points

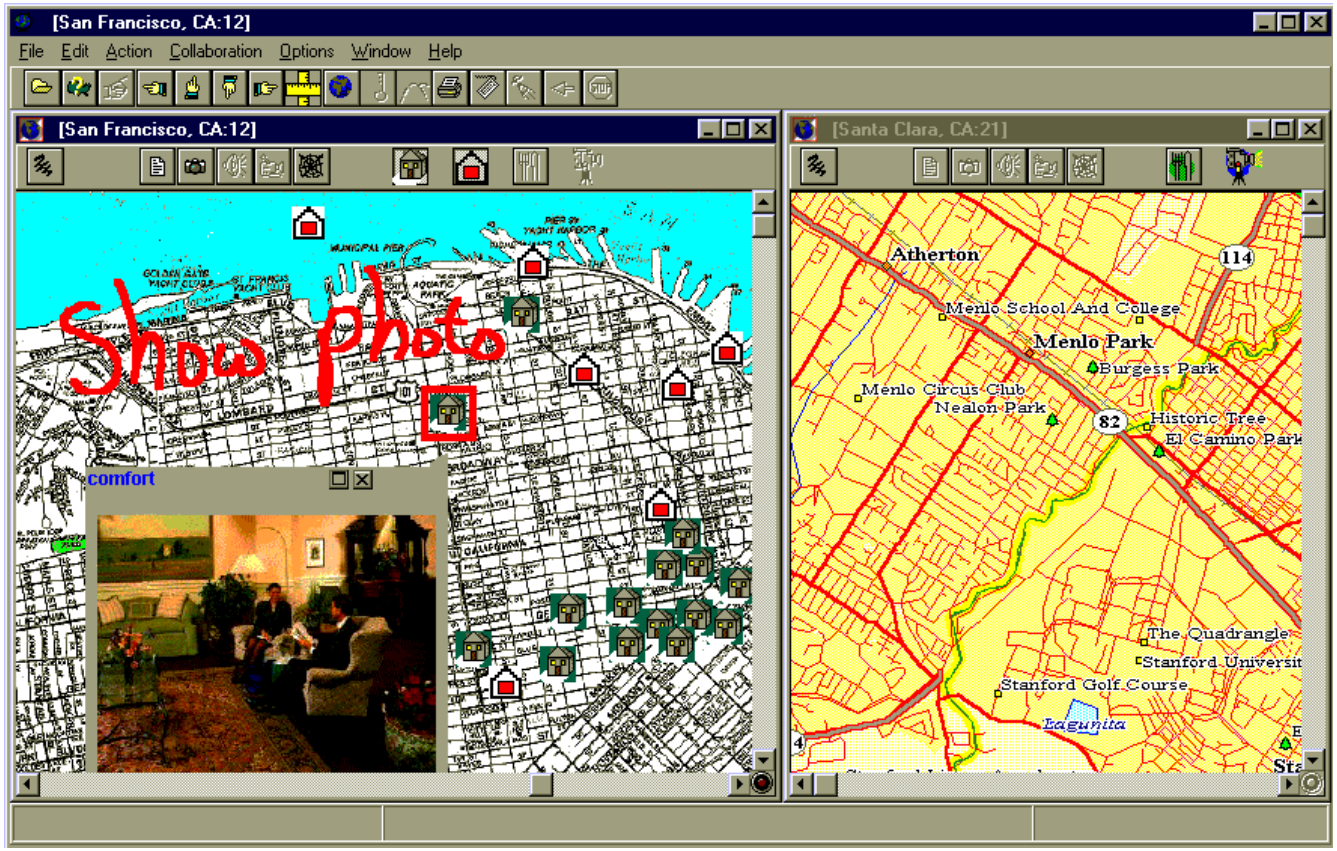
Natural interface to distributed (web) data

Synergistic combination of handwriting, drawing, speech, direct manipulation

Parallel cooperation and competition among many agents

Human & Agent collaboration

Multimodal Maps Application



Main Points

Mobile access to distributed services

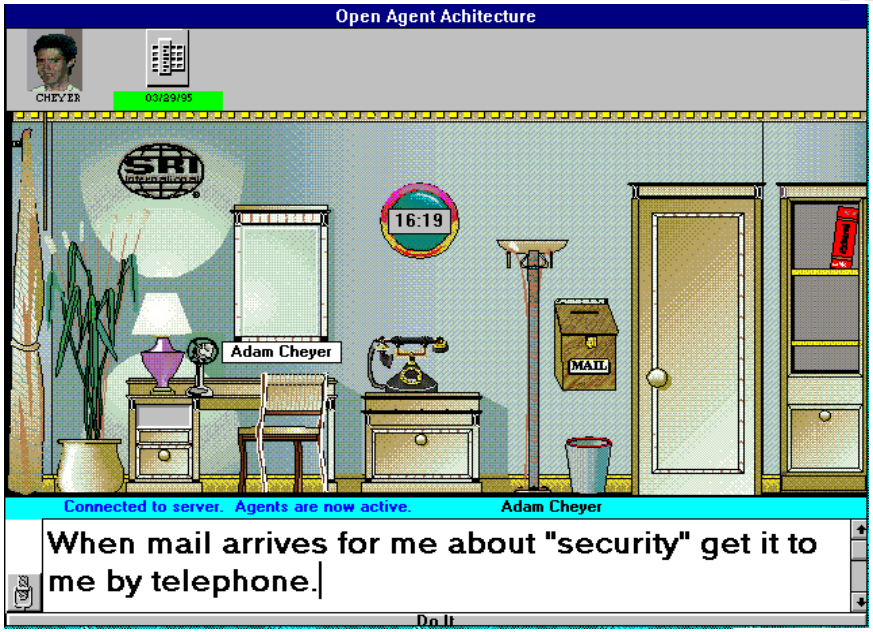
Legacy applications interacting with AI technologies

High-level tasking of agents through NL and speech

Flexible interactions among components

Delegated Triggers

Automated Office Application



Agent-Based Adaptable Interfaces, Coordinated Across Platforms

Multi-Platform

Multimodal User Interfaces

Threats

Malicious Attackers

15-year-old Candaians

HW/SW Faults

Accidental Misconfiguration

Insider Threats

That's All Great, but What About Security?

Mobile Agents

New threats: more capable virus

Autonomous Coordinated Agents

Agents colluding to delude the user

Learning Agents

Highly adaptive adversary in your network

Animated Interface Agents

Someone else's code between you and your computer

Emergent Behavior

New complex global behavior from simple individual agent behavior

Can be good, but could be very dangerous

Threats

- Malicious Hosts
- ePickpockets
- HW/SW Faults
- Accidental Corruption
- Insider Threats

And even if your machine is protected...

What about YOUR agents?

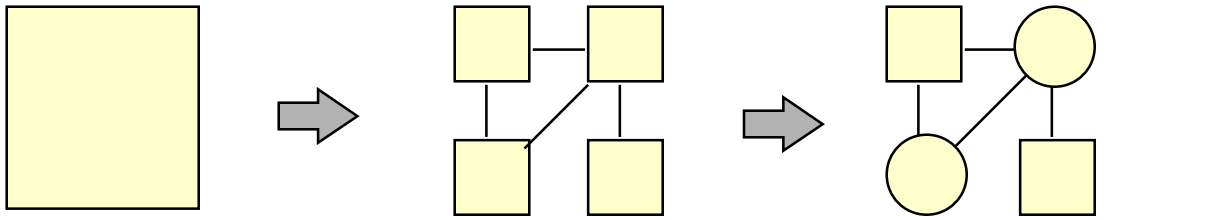
If they go mobile to an untrusted host, are your agents safe?

Can a machine pick your agent's pocket?

Can valuable data, eCash, and authorizations be destroyed, modified, or stolen?

Can emergent behavior of societies of agents interfere with your mission?

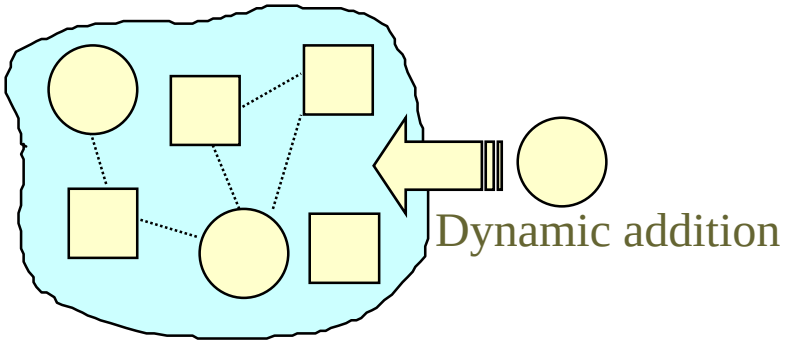
Approaches to Building Agent-Based Applications



Monolithic Applications

Object-Oriented Applications

Distributed Object Applications



Agent-Based Applications

Objective

Virtual community of dynamic services

Adaptable to changing, evolving network resources

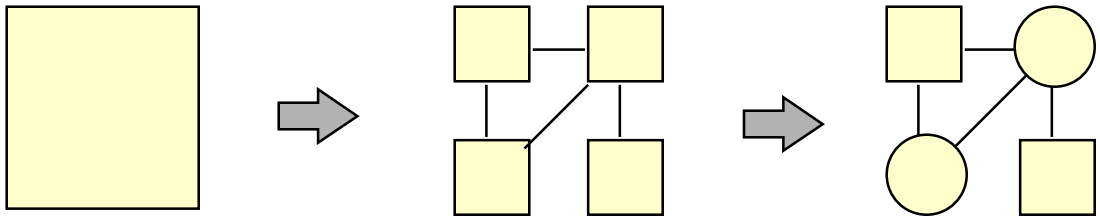
Flexible interactions among components

Approaches to Building Secure Agent-Based Applications

Objective

Trusted virtual community of dynamic services

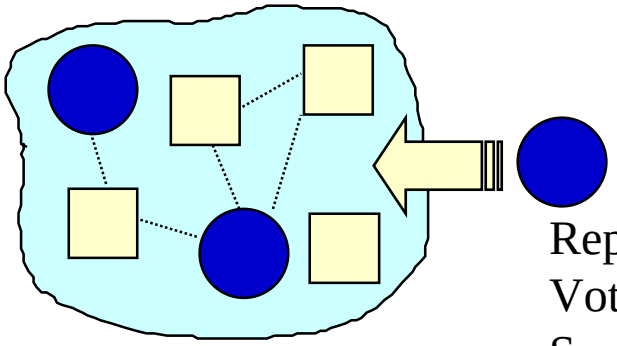
Adaptable to changing, evolving network resources with assurance



Monolithic Applications

Object-Oriented Applications

Distributed Object Applications



Secure Agent-Based Applications

Replication
Voting
Secret-Sharing
Program-Checking

Agent Types

Some agents are replicated

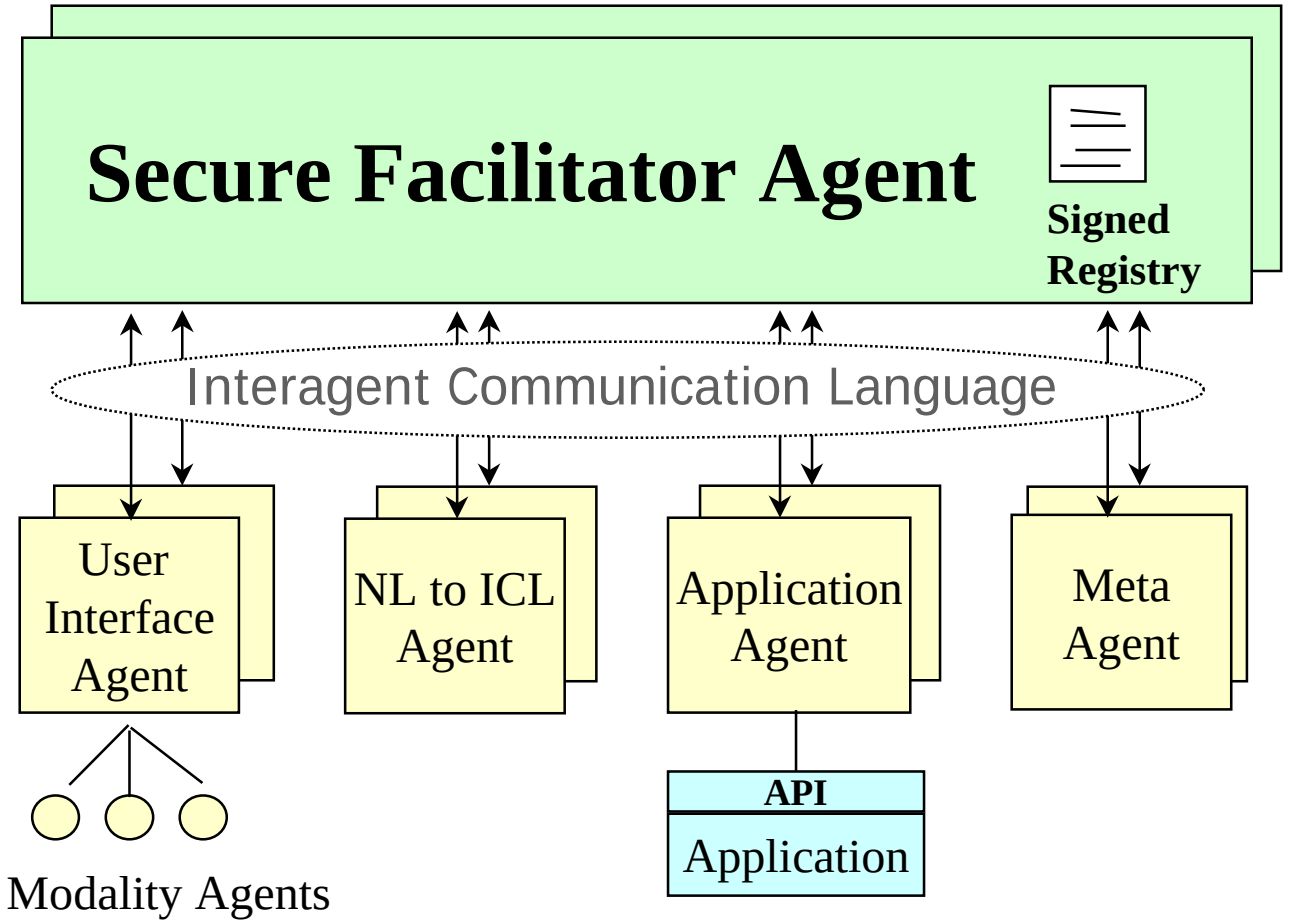
Some secrets are shared

Some Agent communication is signed, encrypted

Facilitator Agents receive ICL requests and coordinate multiagent execution

Meta Agents help coordinate other agents, monitor emergent properties

A Secure Interagent Architecture



Summary

Agent Futures	agents are coming agents add new security risks
Modern Logic, Cryptography	with modern cryptographic primitives and recent logic-based approaches to type systems, secure agent architecture is possible
Government-Sponsored Research	information assurance and related research programs at DARPA, NSA, ONR, NSF, and elsewhere are building the foundations for secure, more highly mobile agent infrastructure
Beneftis	a secure agent infrastructure enables new and better highly assured information infrastructures